Remarks

Claims 1-87 are pending and stand rejected under 35 USC 103(a). Applicants have hereby amended claims 1, 14, 25, 36, 43, 49, 60, 69, 78, and 84, and assert that all claims are now in condition for allowance as more specifically set forth below.

Interview Summary

The undersigned participated in a telephone interview with the Examiner on July 6, 2004. During this interview, the undersigned discussed perceived differences between Ennis and Tams relative to claims 1-87 and in particular the difference between traffic logs as claimed and the packet counts disclosed in Ennis and Tams. Specifically, it was pointed out that a traffic log contains data values detected from an individual packet, while the probe messages of Ennis and Tams instead contain counts of packets that do not provide information relative to an individual packet. While no specific agreement regarding the claims was reached, it was agreed that a reply would be submitted to amend the claims to further clarify that traffic logs contain values determined from an individual packet.

103 Rejections

The Office Action has rejected claims 1-87 as being unpatentable over Ennis (US Pat 5,867,483) in view of Tams (US Pat 6,327,620). Applicants hereby traverse these rejections.

Claims 1-13

In relation to claim 1, the Office Action has stated that Ennis discloses all of the elements except updating the histogram file using the time of creation of a traffic log and at least one of network entry and exit points. However, the Office Action has asserted that Tams discloses updating the histogram file using the time of creation of a traffic log and at least one of network entry and exit points.

Applicants respectfully disagree with this rejection. In particular, applicants disagree that Ennis and Tams disclose the use of traffic logs. Rather, Ennis and Tams utilize probes that count packets and then return a message to a console summarizing the

packet counts. (For example, see FIGS 3-6 and related discussion of Ennis and FIGS. 3-6B and related discussion of Tams.) The console then generates a graph based on the packet counts for a particular period of time. There are no values specific to a particular packet being returned to the console. Therefore, the console cannot analyze data on a packet-by-packet basis, but may only generate graphs based on the limited packet count information provided by the probes.

In contrast, amended claim 1 recites that a traffic log is generated at a first location based upon detection of a packet and the traffic log contains a plurality of values detected from the packet including the network entry and exit points of the packet. Furthermore, the packet is transferred from a first location to a second location where it is stored and thereafter analyzed to determine the time of creation and the entry and exit points of the packet so that the histogram file can be updated accordingly. Once at the second location, knowledge independent of the traffic log is not necessary to determine the path of the packet since this information can be determined from the values of the traffic log, in particular the network entry and exit points.

Neither Ennis nor Tams provides for these claimed features. There is no data detected from a single packet that is collected in Ennis or Tams that is then transferred to another location where it is then analyzed to update a histogram file. Furthermore, there must be knowledge independent of the packet counts in order to determine the path of the packets. For example, the console of Ennis must have independent knowledge that all packets counted by a particular probe correspond to a given network path. Thus, Ennis must keep track of which counts are received from which probes since there are no traffic logs on a per packet basis to inform the console of the path of each individual packet.

Because Ennis and Tams each lack these features recited in claim 1, the combination of Ennis and Tams fails to disclose all of the elements of claim 1. Therefore, claim 1 is patentable over Ennis in view of Tams. Claims 2-13 depend from claim 1 and are also allowable for at least the same reasons. In addition, claims 2-13 recite further features not disclosed or suggested by Ennis in view of Tams.

For example, claim 6 recites that the traffic log can be analyzed to determine the state of a particular packet, which of course requires that the traffic log contain a value relevant to the state of an individual packet. Ennis and Tams do not provide any data

relevant to an individual packet, including the state of each packet. Thus, claim 6 is allowable over this combination of references for this additional reason.

Claims 14-24

As with claim 1, claim 14 as amended recites that the traffic logs be generated at a first location and contain values pertaining to an individual packet, including the network entry and exit points and that the traffic log be transferred to a second location where they are stored and thereafter analyzed to update a histogram file. Thus, the arguments previously presented for claim 1 also apply for claim 14. Additionally, claim 14 recites that a determination be made by analyzing the values of the traffic log as to whether a particular node falls within the path of the packet and that the histogram file for the node be updated only when the node does fall within the path of the packet.

Because neither Ennis nor Tams teaches a traffic log that is transferred to a second location for analysis with entry and exit points stored for a particular packet, neither Ennis nor Tams provides for the determination at the second location of whether the node falls within the path of the packet. Again, Ennis and Tams must rely on independent knowledge of what path a probe is measuring to determine whether a particular probe count applies to a particular path. Therefore, claim 14 is allowable over Ennis and Tams for this additional reason. Claims 15-24 depend from claim 14 and are also allowable for at least the same reasons.

Claims 25-35

As with claims 1 and 14, claim 25 as amended recites that the traffic logs be generated at a first location and contain values pertaining to an individual packet, including the network entry and exit points and that the traffic log be transferred to a second location where they are stored and thereafter analyzed to update a histogram file. Thus, the arguments previously presented for claim 1 also apply for claim 25. Additionally, claim 25 recites that a determination be made by analyzing the values of the traffic log as to whether a particular link falls within the path of the packet and that the histogram file for the link be updated only when the link does fall within the path of the packet.

Because neither Ennis nor Tams teaches a traffic log that is transferred to a second location for analysis with entry and exit points stored for a particular packet, neither Ennis nor Tams provides for the determination at the second location of whether the link falls within the path of the packet. Again, Ennis and Tams must rely on independent knowledge of what path a probe is measuring to determine whether a particular probe count applies to a particular path. Therefore, claim 25 is allowable over Ennis and Tams for this additional reason. Claims 26-35 depend from claim 25 and are also allowable for at least the same reasons.

Claims 36-42

As with the previous claims, claim 36 recites that a traffic log includes values detected for an individual packet. Additionally, claim 36 recites that there be a detection of when a new traffic log is available at a control center and that is it downloaded to a server where it is analyzed to determine the values for the packet that are then used to update a histogram file accordingly. The updated histogram file is then made available to a client computer from the server computer.

As previously discussed, Ennis and Tams fail to disclose the use of traffic logs that contains values for a particular packet. Therefore, there can be no detection of when such a new traffic log is available nor can there be a downloading of such a traffic log to a server where it is analyzed to update a histogram file based on the values for a particular packet. For at least these reasons, claim 36 is allowable over the cited combination. Claims 37-42 depend from claim 36 and are allowable for at least the same reasons.

Claims 43-48

As with the previous claims, claim 43 recites that a traffic log includes values detected for an individual packet and also requires that a plurality of traffic logs be analyzed to generate a histogram based on information about the individual packets stored by the traffic logs. Additionally, claim 43 recites that there be a collection of the traffic logs at a centralized location.

As previously discussed, Ennis and Tams fail to disclose the use of traffic logs where each contains values for a particular packet. Therefore, there can be no analysis of a plurality of such traffic logs to generate a plurality of histograms, nor can there be a centralized collection of such traffic logs. For at least these reasons, claim 43 is allowable over the cited combination. Claims 44-48 depend from claim 43 and are allowable for at least the same reasons.

Claims 49-59

Much like claim 1, claim 49 recites that traffic logs each contain a plurality of values detected from a packet including the network entry and exit points and recites that the traffic logs are analyzed to determine time of creation and network entry and exit points which may be used to update a histogram file. Furthermore, this claim recites that the traffic logs be collected at a network control center and that a computer create and update the histogram file, as well as store and analyze the traffic logs.

As Ennis and Tams fails to disclose the use of traffic logs where each contains values for a particular packet, there can be no network control center that collects such traffic logs nor a computer that stores and analyzes them to update a histogram file. Therefore, claim 49 is allowable over the cited references. Claims 50-59 depend from claim 49 and are also allowable for at least the same reasons. .

Claims 60-68

Much like claim 14, claim 60 recites that a traffic log contains a plurality of values detected from a packet but further recites that a server stores the traffic log, analyzes it, determines a network path of the packet, and updates a histogram of a node when the node falls within the path.

Since Ennis and Tams fail to disclose such a traffic log that contains values about an individual packet, they also fail to disclose a server that stores and analyzes a traffic log to determine whether a node falls within the path of that packet and that updates a histogram for the node only when the node does fall within the path. Therefore, claim 60 is allowable over the cited references. Claims 61-68 depend from claim 60 and are allowable for at least the same reasons. .

Claims 69-77

Much like claim 25, claim 69 recites that a traffic log contains a plurality of values detected from a packet but further recites that a server is programmed to store the traffic logs, analyze each one to determine the path of the corresponding packet, determine whether a link falls within the path, and update a histogram of the link if the link does fall within the path.

Since Ennis and Tams fail to disclose such a traffic log that contains values about an individual packet, they also fail to disclose a server that stores and analyzes a traffic log to determine whether a link falls within the path of that packet and that updates a histogram for the link only when the link does fall within the path. Therefore, claim 69 is allowable over the cited references. Claims 70-77 depend from claim 69 and are allowable for at least the same reasons.

Claims 78-83

Much like claim 36, claim 78 recites that a traffic log contains a plurality of values detected from a packet but further recites that a server detects when new traffic logs are available at a network control center, downloads the traffic logs, and updates the histogram file by analyzing the traffic logs to determine the values detected from the corresponding individual packets.

Again, since Ennis and Tams fail to disclose such a traffic log that contains values about an individual packet, they also fail to disclose a server that detects when new traffic logs are available at a network control center, that downloads the traffic logs, and that updates the histogram file by analyzing the traffic logs. Therefore, claim 78 is allowable over the cited references. Claims 79-83 depend from claim 78 and are allowable for at least the same reasons.

Claims 84-87

Like the previous claims, claim 84 recites that a traffic log contains values detected from and individual packet but also recites that there is a traffic log database that

a computer may access to download the traffic logs and to analyze them to determine the values from the packets and to generate a plurality of histograms.

Ennis and Tams fail to disclose such a traffic log that contains values about an individual packet, they also fail to disclose a database including such traffic logs and a computer that downloads the traffic logs from the database to analyze them when generating histograms. Therefore, claim 84 is allowable over the cited references. Claims 85-87 depend from claim 84 and are allowable for at least the same reasons.

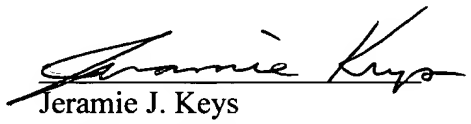
Conclusion

Applicants assert that the application including claims 1-87 is now in condition for allowance. Applicants request reconsideration in view of the amendments and remarks above and further request that a Notice of Allowability be provided. Should the Examiner have any questions, please contact the undersigned.

No fees are believed due. However, please charge any additional fees or credit any overpayment to Deposit Account No. 50-3025.

Respectfully submitted,

Date: July 7, 2004



Jeramie J. Keys
Reg. No. 42,724

Withers & Keys, LLC
P.O. Box 71355
Marietta, Ga 30007-1355
(404) 849.2093